ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS (213113)
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
shawnw@rgrdlaw.com
– and –
FRANK J. JANECEK, JR. (156306)
CHRISTOPHER COLLINS (189093)
655 West Broadway, Suite 1900
San Diego, CA 92101-3301
Telephone: 619/231-1058
619/231-7423 (fax)
fjanacek@rgrdlaw.com
ccollins@rgrdlaw.com

Attorneys for Plaintiff

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ROBERT KLEER, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

vs.

CARRIER IQ, INC., HTC CORP. and HTC AMERICA, INC.,

Defendants.

CV 11-06630 HRL

VIA FAX

No.

CLASS ACTION

COMPLAINT FOR VIOLATIONS OF 18 U.S.C. §2510, *ET SEQ.*

DEMAND FOR JURY TRIAL

Plaintiff Robert Kleer ("Kleer" or "Plaintiff"), by his undersigned attorneys, Robbins Geller Rudman & Dowd LLP, on behalf of himself and all similarly situated persons (the "Class," as defined below), brings this action against defendants Carrier IQ, Inc. ("Carrier IQ") and HTC Corp. and HTC America, Inc. ("HTC") (collectively, "Defendants") and alleges:

NATURE OF THE ACTION

1. This class action complaint seeks monetary and equitable relief pursuant to the Federal Wiretap Act, 18 U.S.C. §2510, *et seq.* (the "Federal Wiretap Act").

2. To put the size of the case in perspective, consider that Carrier IQ preinstalled its software in over 141 million mobile devices. This software enables Defendants to unlawfully access, intercept, and/or collect personal electronic communications and information (*e.g.*, customer location, Internet web searches, content of text messages, etc.) obtained from private mobile devices, including mobile phones, handsets, and smartphones ("Mobile Devices") belonging to Plaintiff and members of the Class. As a result, everything and anything a Mobile Device user types could be logged and analyzed. As alleged herein, the Defendants violated the Federal Wiretap Act by covertly accessing, intercepting, and/or collecting personal electronic communications and information belonging to customers using the Defendants' Mobile Devices.

3. Recently, a Connecticut technology officer, Trevor Eckhart ("Eckhart"), discovered and posted on his blog that Carrier IQ software is clandestinely logging and transmitting private and sensitive information from consumers' Mobile Devices, without the knowledge or consent of the Mobile Device users.[1]

4. On November 30, 2011, the United States Committee on the Judiciary wrote to Carrier IQ demanding responses to inquiries and concerns regarding the software's tracking capabilities and indicating that Carrier IQ's actions "may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act." In addition,

---

[1] http://androidsecuritytest.com/ (last visited December 6, 2011).

members of the House and Senate have likewise sent their own letters to Carrier IQ voicing similar concerns.

5. Plaintiff and members of the Class own HTC Mobile Devices.

6. HTC, as a manufacturer of Mobile Devices, upon information and belief, sells hundreds of millions of Mobile Devices worldwide on a yearly basis.

7. In connection with the ownership of HTC's Mobile Devices by Plaintiff and the Class, the Defendants, unbeknownst to Plaintiff and the members of the Class, had access to, intercepted, and/or collected their personal electronic information and communications, including inherently private facts.

8. As the current or previous provider of wireless and electronic communication services, HTC was and continues to be prohibited from wrongfully accessing, intercepting, and/or collecting any personal electronic communications and information from Plaintiff and members of the Class.

9. However, Defendants improperly accessed, intercepted, and/or collected personal electronic communications and information belonging to Plaintiff and members of the Class. Specifically, HTC caused Carrier IQ to be preinstalled in its Mobile Devices and used it to access, intercept, and/or collect personal electronic communications and information belonging to Plaintiff and the Class.

10. This suit seeks equitable relief and damages on behalf of Plaintiff and the Class.

INTRADISTRICT ASSIGNMENT

11. Defendant Carrier IQ is headquartered in Santa Clara county and a substantial part of the events or omissions which give rise to the claims in this action occurred in the county of Santa Clara, and as such this action is properly assigned to the San Jose division of this Court.

JURISDICTION AND VENUE

12. The Court has original jurisdiction over this matter pursuant to 28 U.S.C. §1331 because this action arose under federal law, specifically, the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Federal Wiretap Act.

13. Furthermore, the Court has original jurisdiction over this matter, pursuant to 28 U.S.C. §1332(d), in that the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action of more than 100 potential Class members in which the citizenship of at least one proposed Class member is different from that of at least one defendant.

14. Venue properly lies in this District pursuant to 28 U.S.C. §1391(a), because certain of the Defendants reside, are found, have an agent, or have transacted substantial business within the Northern District of California within the meaning of 28 U.S.C. §1391(a) as defined in 28 U.S.C. §1391(c), and because a substantial part of the events giving rise to the claims alleged herein occurred in the District.

PARTIES

15. Plaintiff Robert Kleer is a resident of Woodmere, New York. Defendants had access to Plaintiff's personal electronic communications and information through his ownership of an HTC Mobile Device. Plaintiff has owned and used his HTC Incredible since 2010. Plaintiff has not consented to the use of his private/sensitive information, as alleged herein, by Defendants.

16. Carrier IQ, a provider of mobile services intelligence solutions, is a privately owned company headquartered in Mountain View, California, with additional offices in Chicago, Boston, London (UK) and Kuala Lumpur (Malaysia). In October 2010, VisionMobile announced Carrier IQ had joined the "100 Million Club" with its software installed on 100 million phones.[2]

17. Defendant HTC Corp. is a Taiwanese corporation with its North American headquarters in Bellevue, Washington.

18. Defendant HTC America, Inc. is a Washington corporation, with its principle place of business in Bellevue, Washington.

SUBSTANTIVE ALLEGATIONS

19. At all relevant times, Plaintiff owned and continues to own a Mobile Device manufactured by HTC, one of the manufacturers that utilizes the Carrier IQ software.

---

[2] http://markets.financialcontent.com/stocks/news/read?GUID=15163121 (last visited December 6, 2011).

20. In connection with the manufacture and sale of HTC's Mobile Devices, Defendants had access to personal electronic communications and information belonging to Plaintiff and Class members. Defendants unlawfully accessed, intercepted, and/or collected the personal electronic communications and information belonging to Plaintiff and members of the Class in violation of those laws designed specifically to protect consumers and the general public.

Carrier IQ

21. At all relevant times, Carrier IQ software, which is embedded in over a 100 million Mobile Devices, was logging information such as location and detailed key strokes without notifying users or allowing them to opt out.

22. Carrier IQ states that its software is deployed in over 150 million devices worldwide. Carrier IQ also states on its website that it

> is unique in the wireless industry because we are the only company embedding diagnostic software in millions of subscribers' phones. And, we are the only ones who add the "IQ" or smarts to the data. This is Actionable Intelligence – information and analysis you can use to identify problems and more importantly, solve them. And, we are a proven leader with millions of handsets deployed with Carrier IQ software inside.[3]

23. Carrier IQ describes itself as the leading provider of "Mobile Service Intelligence" solutions to the wireless industry. Mobile Service Intelligence is the process of analyzing data from phones to give insight into mobile service quality and user behavior.

24. Carrier IQ claims that "[a]s the only embedded analytics company to support millions of devices simultaneously," it gives wireless carriers and handset manufacturers "unprecedented insight into their customers' mobile experience."

25. Carrier IQ describes its Mobile Service Intelligence Platform ("MSIP") as the smart database at the heart of its solution. Carrier IQ's Insight application suite uses data from the MSIP to deliver true Actionable Intelligence, tailored to specific business areas. For example, "it delivers performance information to support the launch of a new phone or service and historical information to understand in detail ***customer behavior and usage patterns***." Carrier IQ's claims on its website

---

[3] http://www.carrieriq.com/overview/index.htm (last visited December 6, 2011).

that its "Insight suite cuts through the complexity to allow [wireless carriers and manufacturers] to focus on critical business issues, create and track Key Performance Indicators (KPIs) and all in the knowledge that ***the data is measured at the point the customer experienced it – in the phone.***"[4]

26. Carrier IQ software has been classified by many as "rootkit" software. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.

27. Carrier IQ's rootkit has been described as "[a] piece of keystroke-sniffing software" which "has been embedded so deeply in millions of . . . Android devices that it's tough to spot and nearly impossible to remove."[5]

28. Eckhart actually created and posted an online video which demonstrates the handful of points that the Carrier IQ software records and logs and is then sent to the company who is interested in this information.[6] The available information demonstrates that Carrier IQ is capable of recording[7]:

- Key in HTCDialer Pressed or Hardware Keys:
- App Opened
- Sms Received
- Screen Off/On
- Call Received
- Media Statistics
- Location Statistics

---

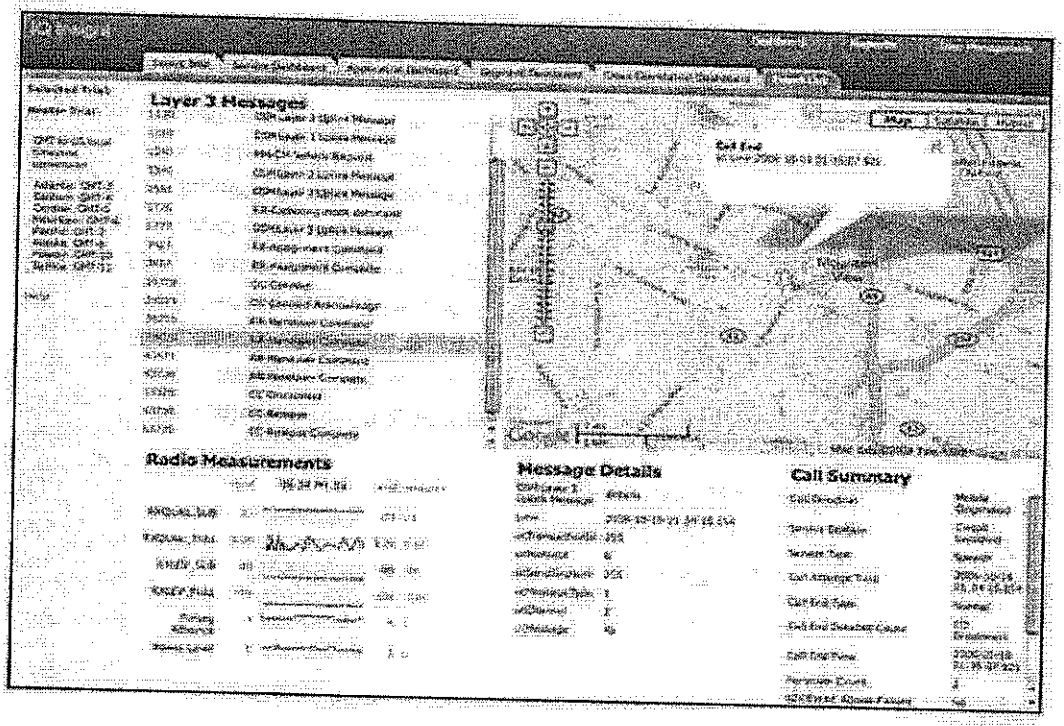
[4] *See* http://www.carrieriq.com/overview/mobileservice/index.htm (last visited on December 2, 2011).

[5] Andy Greenberg, *Phone 'Rootkit' Maker Carrier IQ May Have Violated Wiretap Law In Millions Of Cases*, Forbes, November 30, 2011, available at http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/ (last visited December 6, 2011).

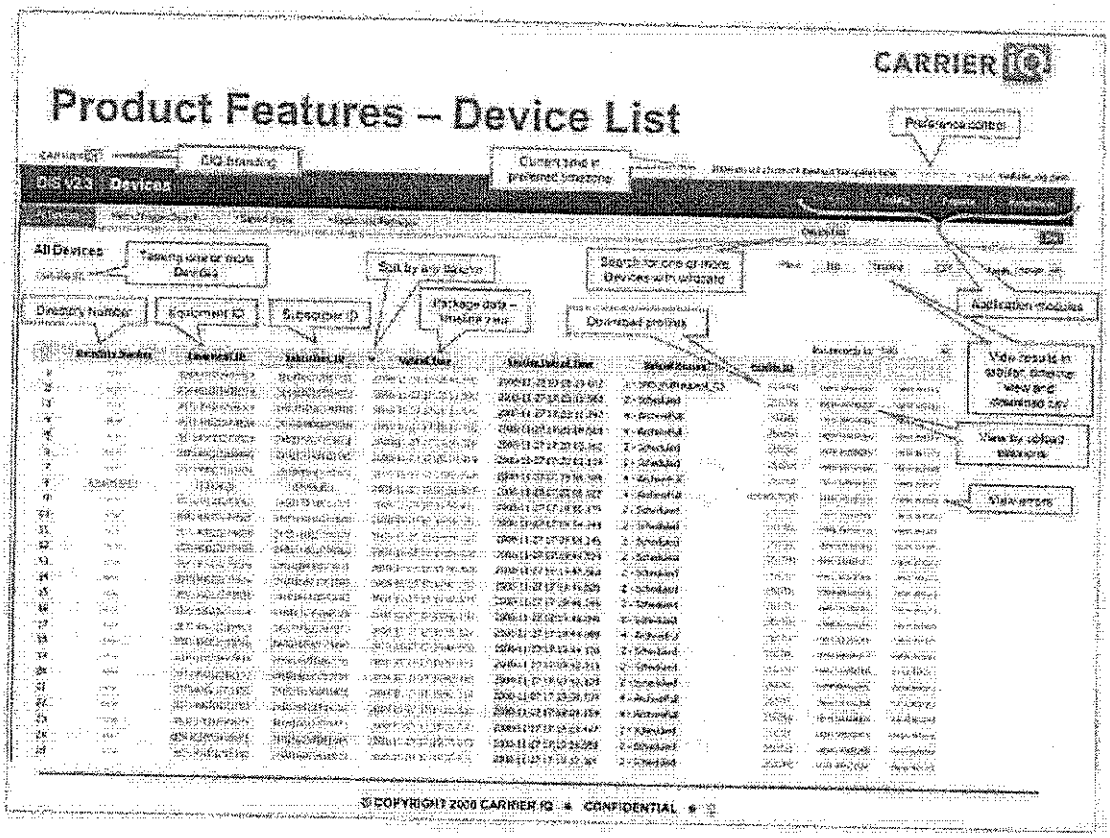
[6] http://www.theregister.co.uk/2011/11/30/smartphone_spying_app/ (last visited December 6, 2011).

[7] http://androidsecuritytest.com/ (last visited December 6, 2011).

29. Eckhart also points out that once the information is obtained from the phone, it is electronically sent to a Carrier IQ web portal. The image below demonstrates the appearance of such a Portal:



30. Another section of the Carrier IQ portal demonstrates the individual types of information that can be requested. For example, the "SMS PullRequest" and the "ArchiveFull" provides information which is sorted by Equipment ID and Subscriber ID and is demonstrated in the Portal as follows:



31. From the Portal, the information can be accessed piece by piece, allowing whoever is using the service to observe the data that was recorded, including the duration of a call alongside its location and radio measurements to help a carrier see what might have happened if a call dropped. *Id.*

32. In fact, Carrier IQ owns a patent that gives them the ability to query just about anything.[8] The patent specifically notes "any user entering data into a browser" as one of the possible functions. *Id.*

HTC and Android Technology

33. HTC, a leading manufacturer of various electronic products, develops and markets a variety of mobile wireless devices and includes the manufacture and sale of "Android" smartphones.

---

[8] http://www.geek.com/articles/mobile/how-much-of-your-phone-is-yours-20111115/ (last visited December 6, 2011)

34. Android is an operating system for mobile devices such as smartphones and tablet computers developed by the Open Handset Alliance, a consortium of 84 hardware, software, and telecommunication companies devoted to advancing open standards for Mobile Devices. The Open Handset Alliance is led by Google.

35. Android has a large community of developers writing applications ("apps") that extend the functionality of the devices. There are currently approximately 400,000 apps available for Android. Apps can be downloaded from third-party sites or through online stores such as Android Market, the app store run by Google.

36. Android was listed as the best-selling smartphone platform worldwide in the 2010 fourth quarter by Canalys, with over 200 million Android devices in use by November 2011.[9]

37. Android apps run in a sandbox, known as an isolated area of the operating system that does not have access to the rest of the system's resources, unless access permissions are granted by the user when the app is installed. Before installing an app, Android Market displays all required permissions. For example, a game may need to enable vibration, but should not need to read messages or access the phonebook. After reviewing these permissions, Android users can decide whether to install the app.

38. Android smartphones also have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build vast databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate smartphones, allowing them to run location-reporting apps (*e.g.*, Foursquare, Latitude, and Places), and to deliver location-based ads.

39. One design issue that has been identified in Android smartphones is that average users cannot monitor how apps access and use private and sensitive data (*e.g.*, location and hardware ID numbers). Even during installation, permission checks do not often indicate to the user how

---

[9] http://digitalprocure.com/index.php?option=com_content&view=article&id=2502:Canalys:-Android-overtakes-Symbian-as-world%27s-best-selling-smartphone-platform-in-Q4-2010-&catid=313&Itemid=10 (last visited on December 6, 2011).

critical services and data will be used or misused. Third-party monitoring software can often identify personal information sent from apps to remote servers.

HTC's Use of the Carrier IQ Software Suite

40. HTC's Android smartphone devices, upon information and belief, are embedded with Carrier IQ software.

41. HTC Android smartphone users have the Carrier IQ software embedded in their Mobile Devices and Defendants have access to their personal electronic communications, information, and other usage data.

42. Upon information and belief, Defendants used the Carrier IQ rootkit software to improperly access, intercept, and/or collect the data containing personal electronic communications and information at the point the mobile user "experienced it" without the mobile user's knowledge or consent.

43. The interception of personal electronic communications and information by the Carrier IQ rootkit likely creates a permanent record of the data. Thereafter, Carrier IQ clients, including HTC and some wireless carriers, have direct access to the personal electronic communications and information of its Mobile Device users.

Concerns over the Interception of Personal Electronic Communications

44. In response to the Eckhart Carrier IQ discovery, Stephen Wicker, a leading expert and Professor at Cornell University, stated "'This is my worst nightmare, . . . [a]s a professor who studies electronic security, this is everything that I have been working against for the last 10 years. It is an utterly appalling invasion of privacy with immense potential for manipulation and privacy theft that requires immediate federal intervention.'"

45. Mobile Device users have a right to not have their personal electronic communications and information, such as content of text messages, content of web searches, phone numbers dialed, URLs visited, and user geographical location accessed, intercepted, and/or collected by third parties.

46. On December 1, 2011, Senator Al Franken, Chairman of the Subcommittee on Privacy Technology and the Law, sent a letter to Carrier IQ's President and Chief Executive Larry Lenhart expressing some concerns over the rootkit's functions. Senator Franken stated:

> I am very concerned by recent reports that your company's software – pre-installed on smartphones used by millions of Americans—is logging and may be transmitting extraordinarily sensitive information from consumers' phones, including:
>
> - when they turn their phones on;
> - when they turn their phones off;
> - the phone numbers they dial;
> - the contents of text messages they receive;
> - the URLs of the websites they visit;
> - the contents of their online search queries – even when those searches are encrypted; and
> - the location of the customer using the smartphone – even when the customer has expressly denied permission for an app that is currently running to access his or her location.
>
> It appears that this software runs automatically every time you turn your phone on. It also appears ***that an average user would have no way to know that this software is running – and that when that user finds out, he or she will have no reasonable means to remove or stop it***.

47. The Senator further explained that he understands "the need to provide usage and diagnostic information to carriers" and that "carriers can modify Carrier IQ's software"; however, "it appears that ***Carrier IQ's software captures a broad swath of extremely sensitive information from users that would appear to have nothing to do with diagnostics*** – including who they are calling, the contents of the texts they are receiving, the contents of their searches, and the websites they visit."

48. According to Senator Franken, "[t]hese actions may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. This is potentially a very serious matter."

49. Mobile Device users are at the mercy of the manufacturers and software developers who have access to their personal electronic communications. Mobile Device users have no ability

to ascertain whether their personal electronic communications are being accessed, and worse, they have no way to stop the improper interception of such communications.

Federal Prohibition on Wiretapping

50. The Federal Wiretap Act provides that "any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished . . . or shall be subject to suit." 18 U.S.C. §2511.

51. Defendants have access to personal electronic communications and other information belonging to Mobile Device users and are subject to the Federal Wiretap Act.

52. Upon information and belief, Defendants violated and continue to violate the Federal Wiretap Act through intercepting, endeavoring to intercept, or procuring other persons to intercept or endeavor to intercept the personal electronic communications and other information belonging to Plaintiff and members of the Class, including, but not limited to: (a) the content of text messages; (b) the content of online searches; (c) the URLs of the websites visited; and (d) the location of the Mobile Device users.

53. The Federal Wiretap Act further provides that:

> [A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter . . . may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.
>
> . . . In an action under this section, appropriate relief includes –
>
> (1) such preliminary and other equitable or declaratory relief as may be appropriate;
>
> (2) damages under subsection (c) and punitive damages in appropriate cases; and
>
> (3) a reasonable attorney's fee and other litigation costs reasonably incurred.
>
> * * *
>
> [T]he court may assess as damages whichever is the greater of –
>
> (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

18 U.S.C. §2520.

54. The Federal Wiretap Act establishes that the Carrier IQ rootkit software, in its present form, is not in compliance with federal law. By itself, the access, interception, and/or collection of personal electronic communications and information, is unlawful and is an invasion or injury to the legally protected privacy interests of Plaintiff and Class members. That compromise to the privacy, confidentiality, and integrity of personal electronic communications and information belonging to the Plaintiff and the Class is actionable under the Federal Wiretap Act.

CLASS ACTION ALLEGATIONS

55. This action is brought as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiff brings this action against Defendants both individually and in a representative capacity as a member of the Class, on behalf of all persons in the United States whose personal electronic communications and information are or were unlawfully intercepted or collected by HTC, its affiliates, or subsidiaries through the use of Carrier IQ software preinstalled on its Android smartphone devices. The Class consists of those persons who were or are owners of HTC Android smartphone devices; subject to any exclusions set forth below (the "Class").

56. Excluded from the Class are Defendants, including any entity in which Defendants have a controlling interest, or which is a parent or subsidiary of, or which is controlled by, any Defendant, and the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, or assigns of any Defendant.

57. The members of the Class are so numerous that joinder of all members is impracticable. The exact number of Class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery. Plaintiff believes, however, that there are, at a minimum, millions of members of the proposed Class, including both current and past HTC Android smartphone users whose personal electronic communications and information were unlawfully accessed, intercepted, and/or collected by the Defendants.

58. Common questions of law and fact exist as to all Class members and predominate over any questions which affect only individual Class members. These common questions of law and fact include:

(a) Whether Defendants have accessed or continue to access, intercept, and/or collect the following personal electronic communications or information in violation of the Federal Wiretap Act: (i) mobile users' location; (ii) mobile users' telephone numbers dialed; (iii) telephone numbers of individuals calling the mobile users; (iv) contents of text messages mobile users receive; (v) contents of text messages mobile users send; (vi) contents of emails mobile users receive; (vii) contents of emails mobile users send; (viii) URLs of the websites that mobile users visit; (ix) contents of the mobile users' online search queries; (x) names and/or contact information from mobile users' address books; and (xi) any other key stroke data;

(b) Whether Defendants transmit the personal electronic communications and information from mobile users phones to Carrier IQ, HTC, wireless carriers, or other third parties;

(c) Whether Defendants use the personal electronic communications or information in violation of the Federal Wiretap Act; and

(d) Whether Plaintiff and the Class have sustained damages, and, if so, the proper measure of damages.

59. Plaintiff's claims are typical of the claims of the Class in that Plaintiff and each Class member sustained, and continue to sustain, damages arising from Defendant's wrongdoing. Plaintiff's damages, as well as the damages of each Class member, were proximately caused by the Defendants' wrongful conduct as alleged herein and were otherwise foreseeable.

60. Plaintiff will fairly and adequately protect the interests of those Class members she seeks to represent and has no interests that are antagonistic to the interests of any other Class member. Plaintiff has retained counsel who have substantial experience and success in complex litigation, including the litigation of class actions and consumer protection claims, and privacy protection claims in the class action context.

61. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, since joinder of all the individual Class members is impracticable.

Furthermore, because the damages suffered, and continued to be suffered, by each individual Class member may be relatively small, the expense and burden of individual litigation would make it very difficult or impossible for individual Class members to redress the wrongs done to each of them individually and the burden imposed on the judicial system would be enormous.

62. In addition, the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

COUNT I

Violation of the Federal Wiretap Act

63. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

64. At all relevant times, Defendants were "communication common carrier[s]" as those terms are used in the Federal Wiretap Act.[10]

65. At all relevant times, Plaintiff and the members of the Class were persons entitled to the protection of the Federal Wiretap Act as Mobile Device users and parties to electronic communications.

66. Upon information and belief, Defendants have intercepted and continue to intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept the substance of the personal electronic communications belonging to Plaintiff and members of the Class.

67. As a proximate result of Defendants' improper interception and/or collection of the personal electronic communications and information, the Class has suffered a legally cognizable loss or injury.

---

[10] *See* 18 U.S.C. §2510; 47 U.S.C. §151.

68. The losses sustained by the Class are directly attributable to Defendants' wrongful conduct and were entirely foreseeable.

PRAYER FOR RELIEF

69. Wherefore, Plaintiff requests the following relief, individually and on behalf of the Class:

A. Certification of this action as a class action, appointment of Plaintiff as a Class representative and the undersigned counsel as Class counsel;

B. An order declaring the actions complained of herein to be in violation of the statutory law set forth above, including a preliminary injunction enjoining Defendants from further acts in violation of the Federal Wiretap Act, pending the outcome of this action;

C. An order enjoining and restraining Defendants from any further acts in violation of the Federal Wiretap Act set forth above;

D. An award of compensatory damages in an amount deemed appropriate by the trier of fact against Defendants;

E. An award of prejudgment and post-judgment interest;

F. An award of costs, including, but not limited to, discretionary costs, attorneys' fees and expenses incurred in prosecuting this case; and

G. Any other and further relief to which Plaintiff and the Class may be entitled at law or in equity that this Court deems just and proper.

JURY DEMAND

Plaintiff and the Class demand a trial by jury on all issues so triable.

DATED: December 23, 2011

ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS

S/ Shawn A. Williams
SHAWN A. WILLIAMS

Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
FRANK J. JANECEK, JR.
CHRISTOPHER COLLINS
655 West Broadway, Suite 1900
San Diego, CA 92101-3301
Telephone: 619/231-1058
619/231-7423 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
SAMUEL H. RUDMAN
ROBERT M. ROTHMAN
MARK S. REICH
ANDREA Y. LEE
58 South Service Road, Suite 200
Melville, NY 11747
Telephone: 631/367-7100
631/367-1173 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
PAUL J. GELLER
STUART A. DAVIDSON
MARK DEARMAN
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

Attorneys for Plaintiff

S:\CptDraft\Consumer\Cpt Carrier IQ (NDCA).doc